UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,474	06/12/2001	Jamal Benbrahim	IGT1P376/P000227-001	5212

79646 7590 04/21/2011

Weaver Austin Villeneuve & Sampson LLP - IGT
Attn: IGT
P.O. Box 70250
Oakland, CA 94612-0250

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
04/21/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@wavsip.com

Office Action Summary	Application No.	Applicant(s)	
	09/880,474	BENBRAHIM, JAMAL	
	Examiner	Art Unit	
	JAMES D. NIGH	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *18,21,22,24-26,28-30,32-38,40,41 and 45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *18,21,22,24-26,28-30,32-38,40,41 and 45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *24 March 2011*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to amendments and remarks filed on 24 March 2011.

Claim Status

2. Claims 18, 22, 35, 36, 37, 38, 40, 41 and 45 have been amended. Claims 1-17 were previously cancelled. Claims 19, 20, 39, 42, 43 and 44 have been cancelled in the present amendment. Claims 18, 21-22, 24-26, 28-30, 32-38, 40-41 and 45 are currently pending and are presented for examination on the merits.

Information Disclosure Statement

3. The information disclosure statement (IDS) was submitted on 24 March 2011. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Definition

4. Jurisdiction: authority of a sovereign power to govern or legislate: power or right to exercise authority, or the limits or territory within which any particular power may be exercised: sphere of authority.

Response to Amendment

5. Claim 18 recites "storing on the gaming device a secure access module, wherein the secure access module includes a private key associated with a local jurisdiction in which the gaming device is located, such that the private key need not be transmitted over a network". Claims 37 and 41 contain a similar recitation. Examiner has reviewed Applicant's disclosure and in particular paragraphs 0031 and 0051. It would appear to

those skilled in the art that the claimed secure access module is physical hardware with an internal processor, encryption/decryption engine and memory per paragraph 0031 which must be installed physically by an operator as disclosed in paragraph 0051. As such it is unclear how a physical component can be stored in a manner akin to data as recited by the claim as the component would be understood by those skilled in the art to be a form of a storage device in view of the disclosure. As such the claim will be held as indefinite.

6. Claim 36 recites "…implementing a secure access module, wherein the secure access module includes the first and second keys such that the first and second keys need not be transmitted over a network". Claim 37 contains a similar recitation. Examiner has thoroughly reviewed Applicant's disclosure and in particular paragraphs 0031 and 0051 and finds no teaching of a secure access module with multiple keys. Therefore this will be treated as new subject matter.

Response to Arguments

7. Applicant's argument with regard to the 35 U.S.C. § 101 rejection of claims 36-39 and 41-44 has been fully considered and is persuasive. Accordingly the rejection will be withdrawn.

8. Applicant's argument with regard to the 35 U.S.C. § 112, 1st paragraph rejection of claim 37 with regard to the step of "determining which one of a plurality of encrypted blocks of game code is to be executed…" has been fully considered but is not persuasive. As indicated in Applicant's remarks "…then the *gaming device with a certain secure access module must determine* which block of code it can decrypt, given

its specific secure access module and key" (Examiner emphasis added). However according to the order of claim 37 the determination is being made prior to the step of "storing on the gaming device a secure access module...". Thus per the claim no secure access module is resident on the gaming device at the point where the step of determining is taking place. As such no decryption keys would be resident on the gaming device; therefore it would not be possible to make the claimed determination without the secure access module which is required by the claim. Stated differently the sequence of steps cannot be performed in the order recited as the element necessary to make the determination i.e. the secure access module is not recited as being present at the time when the determination is being made and is only claimed as being present in a subsequent step. Therefore Examiner maintains that the claims as recited are not enabled.

9. Applicant's argument with regard to the 35 U.S.C. § 112, 1st paragraph rejection of claim 40 with regard to the step of "determining which one of a plurality of encrypted blocks of game code is to be executed…" has been fully considered but is not persuasive. As noted in Applicant's remarks regarding claim 37, the determination is taking place by virtue of the decryption operation disclosed in paragraph 0051. However this operation is disclosed as being performed at a gaming machine when a SAM is installed and as noted by Applicant's remarks "…then the *gaming device* with a certain secure access module must determine which block of code it can decrypt, given its specific secure access module and key. By virtue of having a secure access module containing a key for decrypting a specific portion or block of code/data from a group of

code, the *gaming device* necessarily determines which block it can decrypt because the determined block is the only block the gaming device can decrypt, given its secure access module" (Examiner emphasis added). No operation of determining which one of a plurality of encrypted blocks of game code is to be executed is disclosed as taking place at a gaming server as claimed. Therefore the rejection that this is new subject matter will be maintained. In addition the remarks will be used as the basis for a 35 U.S.C. § 112, 2nd paragraph rejection of claim 40 as provided by MPEP § 2172 "Evidence that shows that a claim does not correspond in scope with that which applicant regards as applicant's invention may be found, for example, in contentions or admissions contained in briefs or remarks filed by applicant", *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 55 USPQ2d 1279 (Fed. Cir. 2000); *In re Prater*, 415 F.2d 1393, 162 USPQ 541 (CCPA 1969)

10. Applicant's argument with regard to the 35 U.S.C. § 112, 1st paragraph rejection of claim 37 with regard to the step of "attempting to authenticate the information…" has been fully considered but is not persuasive. The claim only recites the gaming device and no other device. The disclosure in paragraph 0058 recites "In one or more embodiments, the decrypted data may be transmitted to a remote source for authentication". Thus no teaching has been provided of authentication or even an attempt to authenticate information taking place at the gaming device. Therefore Examiner maintains that a recitation of attempting to authenticate occurring at the gaming device constitutes new subject matter. As such the rejection will be maintained.

11. Applicant's argument with regard to the 35 U.S.C. § 112, 1st paragraph rejection of claim 40 with regard to the step of "attempting to authenticate the information…" has been fully considered and is persuasive. Accordingly the rejection will be withdrawn.

12. Applicant's argument with regard to the 35 U.S.C. § 112, 1st paragraph rejection of claim 38 has been fully considered but is not persuasive. Claim 38 is dependent upon claim 37 which only claims a single "computer" as performing the steps as recited by the preamble. The limitations of claim 37 only recite a gaming device as the particular machine performing the method steps which Examiner is therefore interpreting to be the single computer recited in the preamble. If this is indeed the case then as recited in claim 38 the gaming device would be sending encrypted executable code to itself as it is the only recited machine in claim 37 or 38. Examiner can find no recitation within the disclosure of the gaming device sending encrypted executable code to itself as would be indicated by the claim. Therefore Examiner maintains that such a step does not find support within the disclosure and is therefore new subject matter. As such the rejection will be maintained.

13. Applicant's argument with regard to the 35 U.S.C. § 112, 2nd paragraph rejection of claims 18, 22, 35, 36, 37, 40, 41 and 45 regarding "receiving from a remote device…" has been fully considered and is persuasive. Accordingly the rejection will be withdrawn.

14. Applicant's arguments with regard to the 35 U.S.C. § 112, 2nd paragraph rejection of claim 18 regarding "taking remedial action…" has been fully considered and is persuasive. Accordingly the rejections will be withdrawn.

15. Applicant's argument with regard to the 35 U.S.C. § 103 (a) rejection of claim 18 as being obvious over Rowe in view of Hind and in further view of Alcorn has been fully considered but is moot in view of the new ground(s) of rejection. However Examiner wishes to comment on Applicant's remarks. Examiner notes that multiple games are not stored merely at the GTDR but also at the gaming terminal as disclosed by Rowe in column 9, lines 21-34. Therefore Rowe does disclose "receiving at the gaming device...executable code of a plurality of games...including a first game...and second game". Examiner would also point out that with regard to the Graunke reference and the amended language regarding the key not needing to be transmitted over a network as claimed in the amended language that the argument is now moot.

Claim Rejections - 35 USC § 112

16. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

17. Claims 36-38 and 40 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

18. Claim 36 recites "…implementing a secure access module, wherein the secure access module includes the first and second keys such that the first and second keys need not be transmitted over a network". Claim 37 contains a similar recitation.

Examiner has thoroughly reviewed Applicant's disclosure and in particular paragraphs 0031 and 0051 and finds no teaching of a secure access module with multiple keys. Therefore this will be treated as new subject matter.

19. Claim 37 recites "attempting to authenticate the information…" The claim only recites the gaming device and no other device. The disclosure in paragraph 0058 recites "In one or more embodiments, the decrypted data may be transmitted to a remote source for authentication". Thus no teaching has been provided of authentication or even an attempt to authenticate information taking place at the gaming device. Therefore Examiner maintains that a recitation of attempting to authenticate occurring at the gaming device constitutes new subject matter.

20. Claim 38 is dependent upon claim 37 which only claims a single "computer" as performing the steps as recited by the preamble. The limitations of claim 37 only recite a gaming device as the particular machine performing the method steps which Examiner is therefore interpreting to be the single computer recited in the preamble. If this is indeed the case then as recited in claim 38 the gaming device would be sending encrypted executable code to itself as it is the only recited machine in claim 37 or 38. Examiner can find no recitation within the disclosure of the gaming device sending encrypted executable code to itself as would be indicated by the claim. Therefore Examiner maintains that such a step does not find support within the disclosure and is therefore new subject matter.

21. Claim 38 is also rejected as being dependent upon claim 37.

22. Claim 40 recites "determining which one of a plurality of encrypted blocks of game code is to be executed…" As noted in Applicant's remarks regarding claim 37, the determination is taking place by virtue of the decryption operation disclosed in paragraph 0051. However this operation is disclosed as being performed at a gaming machine when a SAM is installed and as noted by Applicant's remarks "…then the *gaming device* with a certain secure access module must determine which block of code it can decrypt, given its specific secure access module and key. By virtue of having a secure access module containing a key for decrypting a specific portion or block of code/data from a group of code, the *gaming device* necessarily determines which block it can decrypt because the determined block is the only block the gaming device can decrypt, given its secure access module" (Examiner emphasis added). No operation of determining which one of a plurality of encrypted blocks of game code is to be executed is disclosed as taking place at a gaming server as claimed. Therefore this represents new subject matter.

23. Claims 37-38 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

24. Claim 37 recites "determining which one of a plurality of encrypted blocks of game code is to be executed…" As indicated in Applicant's remarks "…then the *gaming device with a certain secure access module must determine* which block of code it can

decrypt, given its specific secure access module and key" (Examiner emphasis added). However according to the order of claim 37 the determination is being made prior to the step of "storing on the gaming device a secure access module...". Thus per the claim no secure access module is resident on the gaming device at the point where the step of determining is taking place. As such no decryption keys would be resident on the gaming device; therefore it would not be possible to make the claimed determination without the secure access module which is required by the claim. Stated differently the sequence of steps cannot be performed in the order recited as the element necessary to make the determination i.e. the secure access module is not recited as being present at the time when the determination is being made and is only claimed as being present in a subsequent step. Therefore the claims as recited are not enabled.

25. Claim 38 is also rejected as being dependent upon claim 37.

26. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

27. Claims 18, 21 37-38 and 41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

28. Claim 18 recites “storing on the gaming device a secure access module, wherein the secure access module includes a private key associated with a local jurisdiction in which the gaming device is located, such that the private key need not be transmitted over a network”. Claims 37 and 41 contain a similar recitation. Examiner has reviewed Applicant’s disclosure and in particular paragraphs 0031 and 0051. It would appear to

those skilled in the art that the claimed secure access module is physical hardware with an internal processor, encryption/decryption engine and memory per paragraph 0031 which must be installed physically by an operator as disclosed in paragraph 0051. As such it is unclear how a physical component can be stored in a manner akin to data as recited by the claim as the component would be understood by those skilled in the art to be a form of a storage device in view of the disclosure. As such the claim will be held as indefinite. For purposes of claim interpretation the claim will recite "implementing on the gaming device a secure access module".

29. Claim 21 is also rejected as being dependent upon claim 18.

30. Claim 38 is also rejected as being dependent upon claim 37.

31. **Claim 40 rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention.**

32. Evidence that claim 40 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed 24 March 2011. In that paper, applicant has stated "...then the *gaming device* with a certain secure access module must determine which block of code it can decrypt, given its specific secure access module and key. By virtue of having a secure access module containing a key for decrypting a specific portion or block of code/data from a group of code, the *gaming device* necessarily determines which block it can decrypt because the determined block is the only block the gaming device can decrypt, given its secure access module", and this statement indicates that the invention is different from what is defined in the claim(s) because no operation of determining which one of a plurality of encrypted blocks of

game code is to be executed is disclosed as taking place at a gaming server as claimed. "Evidence that shows that a claim does not correspond in scope with that which applicant regards as applicant's invention may be found, for example, in contentions or admissions contained in briefs or remarks filed by applicant", *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 55 USPQ2d 1279 (Fed. Cir. 2000); *In re Prater*, 415 F.2d 1393, 162 USPQ 541 (CCPA 1969)

Claim Rejections - 35 USC § 103

33. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

34. Claims 18, 21-22, 24-26, 29-30, 33-38, 40 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowe (U.S. Patent 6,645,077, hereinafter referred to as Rowe) in view of Hind et al. (U.S. Patent 6,978,367, hereinafter referred to as Hind) and in view of Alcorn et al. (U.S. Patent 6,149,522, hereinafter referred to as Alcorn) and in further view of Immonen (U.S. Patent 7,382,882, hereinafter referred to as Immonen).

35. As per claims 18 and 36

Rowe discloses receiving from a remote device encrypted executable code for a plurality of games (Abstract, Figure 3, 3:41-51, 5:57-58, 22:31-51)

Rowe discloses that the encrypted executable code includes first game code necessary to operate a game on the gaming device in a first jurisdiction (Figure 3, 13:50-65, 14:7-8)

Rowe discloses that the encrypted executable code includes second game code necessary to operate a game on the gaming device in a second jurisdiction (Figure 3, 13:50-65, 14:7-8)

Rowe discloses wherein the first game code includes a first set of operating data including at least one of first audio data or first video data for generating the game on the gaming device in the first jurisdiction, and wherein the second game code includes a second set of operating data including at least one of second audio data or second video data for generating the game on the gaming device in the second jurisdiction (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Per claim 36 Rowe discloses a computer readable medium (8:35-39).

However Rowe does not explicitly disclose that the first set of code is encrypted with a first key associated with the first jurisdiction. Hind teaches that the first set of code is encrypted with a first key associated with the first jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50) (Examiner views the disclosure of the second and third policies with separate encryption keys and separate communities to be equivalent to "jurisdictions" per the definitions shown above).

Hind teaches that a second set of code encrypted with a second key is associated with a second jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches that the second set of code is not recoverable with the first key and the first set of code is not recoverable with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches wherein when the private key is the first key, and the local jurisdiction is the first jurisdiction, decrypting by the device the first set of code according to the first key to recover the first game code and the first set of operating data as decrypted first set of code and a decrypted first set of operating data, respectively (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches wherein when the private key is the second key, and the local jurisdiction is the second jurisdiction, decrypting by the device the second set of code according to the second key to recover the second set of code and the second set of operating data as decrypted second set of code and decrypted second set of operating data, respectively (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches storing on the device the first set of code, including the first set of operating data, encrypted with the first key and the second set of code, including the second set of operating data, encrypted with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches executing the decrypted first or second set of code on the device using the decrypted first or second set of operating data (37:1-21) (As no definition of "operating data" has been supplied in the claim Examiner views the document of Hind to fall under the broadest reasonable interpretation of the term).

Hind teaches storing the decrypted first or second set of code on the device (37:1-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind explicitly disclose authentication. Alcorn teaches receiving, by the gaming device, results of the authentication from the remote device (9:9-16, 13:14-17)

Alcorn teaches taking remedial action when the authentication fails (9:6-16).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to

modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

Neither Rowe nor Hind or Alcorn explicitly disclose implementing on the gaming device a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. Immonen teaches a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. (6:1-33).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn further with the secure session set up of Immonen for the purpose of satisfying the need to use a mutually agreed master secret for a relatively long time (2:29-30).

However the recitation “wherein when the private key is the first key, and the local jurisdiction is the first jurisdiction, decrypting and storing by the naming device the first game code according to the first key to recover the first game code and the first set of operating data as decrypted first game code and a decrypted first set of operating data, respectively” is not entitled to patentable weight as the steps recited can both be considered optional and are therefore not limiting per MPEP § 2106 II C.

The recitation “wherein when the private key is the second key, and the local jurisdiction is the second jurisdiction, decrypting by the gaming device the second game

code according to the second key to recover the second game code and the second set of operating data as decrypted second game code and decrypted second set of operating data, respectively" is not entitled to patentable weight as the steps recited can both be considered optional and are therefore not limiting per MPEP § 2106 II C.

The recitation "when the decrypted first or second game code is not authenticated by the remote device, wherein the remedial action includes not allowing the decrypted first or second game code to be executed by the gaming device" is not entitled to patentable weight as the steps recited can both be considered optional and are therefore not limiting per MPEP § 2106 II C.

The recitation "wherein the first game code includes a first set of operating data including at least one of first audio data or first video data for generating the game on the gaming device in the first jurisdiction, and wherein the second game code includes a second set of operating data including at least one of second audio data or second video data for generating the game on the gaming device in the second jurisdiction" is not entitled to patentable weight as no additional method step is recited and the "generating" is only suggested but never performed, per MPEP § 2106 II C; moreover as none of the other recited method steps exhibit any dependency on the nature of the game code it is simply analogous to printed matter ""Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability .... [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and

the substrate" *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II.

36. As per claim 21

Rowe further discloses storing game code at the gaming device (9:21-56)

37. As per claims 22 and 35

Rowe discloses a memory device for storing executable code for a plurality of games (9:21-56, 20:1-21)

Rowe discloses that the encrypted executable code includes first game code necessary to operate a game on the gaming device in a first jurisdiction (Figure 3, 13:50-65, 14:7-8)

Rowe discloses that the encrypted executable code includes second game code necessary to operate a game on the gaming device in a second jurisdiction (Figure 3, 13:50-65, 14:7-8)

Rowe discloses wherein the first game code includes a first set of operating data including at least one of first audio data or first video data for generating the game on the gaming device in the first jurisdiction, and wherein the second game code includes a second set of operating data including at least one of second audio data or second video data for generating the game on the gaming device in the second jurisdiction (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Rowe discloses a mechanism for receiving elements of value (20:1-21)

Rowe discloses a mechanism for making a bet (19:28-67)

Rowe discloses a display for displaying the outcome of a game (19:28-67)

Rowe discloses a programmable memory (20:1-21)

Rowe discloses a controller (20:1-21)

Per claim 35 Rowe discloses communication link between the gaming device and the remote device (20:46-60, 21:3-24)

However Rowe does not explicitly disclose that the first set of code is encrypted with a first key associated with the first jurisdiction. Hind teaches that the first set of code is encrypted with a first key associated with the first jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches that a second set of code encrypted with a second key is associated with a second jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches that the second set of code is not recoverable with the first key and the first set of code is not recoverable with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches wherein when the private key is the first key, and the local jurisdiction is the first jurisdiction, decrypting by the device the first set of code according to the first key to recover the first game code and the first set of operating data as decrypted first set of code and a decrypted first set of operating data, respectively (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches wherein when the private key is the second key, and the local jurisdiction is the second jurisdiction, decrypting by the device the second set of code

according to the second key to recover the second set of code and the second set of operating data as decrypted second set of code and decrypted second set of operating data, respectively (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches storing on the device the first set of code, including the first set of operating data, encrypted with the first key and the second set of code, including the second set of operating data, encrypted with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches executing the decrypted first or second set of code on the device using the decrypted first or second set of operating data (37:1-21) (As no definition of "operating data" has been supplied in the claim Examiner views the document of Hind to fall under the broadest reasonable interpretation of the term).

Hind teaches storing the decrypted first or second set of code on the device (37:1-21).

Hind teaches receiving a private key (29:42-51, 29:66-30:12)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind explicitly disclose authentication. Alcorn teaches authentication (Abstract, 2:47-65, 3:37-43, 8:32-9:16)

Alcorn teaches taking remedial action when the authentication fails (9:6-16).

Per claim 35 Alcorn also teaches a remote device receiving information relating to the code (2:47-65).

Per claim 35 Alcorn teaches authenticating the code (2:47-65)

Per claim 35 Alcorn teaches sending a message to the gaming device as to whether the code is authentic (9:9-16).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

Neither Rowe nor Hind or Alcorn explicitly disclose implementing on the gaming device a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. Immonen teaches a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. (6:1-33).

Immonen teaches the capability of decrypting using the private key (7:30-38).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn further with the secure session set up of Immonen for the purpose of satisfying the need to use a mutually agreed master secret for a relatively long time (2:29-30).

The recitations of claims 22 and 35 “operable to…”, “configured to…”, “capable of…” are not entitled to patentable weight as the claims are directed towards an apparatus and do not recite any structural limitations but merely intended use of the structure. See MPEP § 2106 II C, MPEP § 2111.04 and MPEP § 2114.

In addition the recitations regarding the nature of the game code and the operating data are not entitled to patentable weight as these are merely non-functional descriptive material “Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability …. [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate” *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II.

38. As per claim 24

Rowe further discloses wherein the controller includes a processor in communication with the programmable memory (20:1-25).

39. As per claim 25

Rowe further discloses wherein the programmable memory comprises RAM (20:1-21).

40. As per claim 26

Rowe further discloses including a communications link associated with the controller permitting the first set of operating data and the second set of operating data to be transmitted to the gaming device from a remote location (20:46-60).

41. As per claim 29

Rowe discloses game code (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Hind teaches that code is selectively encrypted (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind teaches a digital signature. Alcorn teaches a digital signature (8:59-9:40).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for

decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

However as the claim is directed towards an apparatus the recitation is not limiting as no further structural limitation is being recited per MPEP § 2111.04 and MPEP § 2114.

42. As per claim 30

Rowe discloses game code (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Hind teaches that code is selectively encrypted (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind teaches information relating to the code is sent to the remote device. Alcorn teaches information relating to the code being sent to the remote device (2:47-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution

system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

However as the claim is directed towards an apparatus the recitation is not limiting as no further structural limitation is being recited per MPEP § 2111.04 and MPEP § 2114.

43. As per claim 33

Rowe discloses game code (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Hind teaches that first and second code is selectively encrypted (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind teaches a digital signature. Alcorn teaches a digital signature (8:59-9:40).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution

system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

However as the matching of digital signatures does not depend on the data being of a specific nature but only that the signature be calculated on the same data at both devices, the recitation regarding the data is simply non-functional descriptive material.

44. As per claim 34

Rowe discloses game code (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Hind teaches that code is selectively encrypted (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind teaches information relating to the code is sent to the remote device. Alcorn teaches information relating to the code being sent to the remote device (2:47-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

However as the matching of digital signatures does not depend on the data being of a specific nature but only that the signature be calculated on the same data at both devices, the recitation regarding the data is simply non-functional descriptive material.

45. As per claims 37 and 40

Rowe discloses determining which one of a plurality of encrypted blocks of game code is to be executed by a gaming device (5:57-58, 8:23-39, 12:34-47, 13:58-65, claim 1) (Examiner notes that no specific definition of the term “blocks of game code” is contained within the claim, therefore in the broadest reasonable interpretation an entire game can be construed as “blocks of game code”)

Rowe discloses that the encrypted executable code includes first game code necessary to operate a game on the gaming device in a first jurisdiction (Figure 3, 13:50-65, 14:7-8)

Rowe discloses that the encrypted executable code includes second game code necessary to operate a game on the gaming device in a second jurisdiction (Figure 3, 13:50-65, 14:7-8)

Rowe discloses a computer readable medium (8:35-39).

However Rowe does not explicitly disclose that the first set of code includes code necessary to operate in a first venue. Hind teaches that the first set of code is encrypted with a first key necessary to operate in a first venue (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50) (Examiner views the disclosure of the second and third policies with separate encryption keys and separate communities to be equivalent to "jurisdictions" per the definitions shown above).

Hind teaches that a second set of code encrypted with a second key unnecessary to operate in the first venue and necessary to operate in a second venue (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches that the second set of code is not decryptable with the first key and the first set of code is not decryptable with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind explicitly disclose receiving information from the gaming device. Alcorn teaches a remote device receiving information relating to the code (2:47-65).

Alcorn teaches authentication of the code (Abstract, 2:47-65, 3:37-43, 8:32-9:16)

Alcorn teaches sending a message to the gaming device as to whether the code is authentic (9:9-16).

Alcorn teaches indicating that the code is not to be executed when the code is not authentic (9:6-16).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

Neither Rowe nor Hind or Alcorn explicitly disclose implementing on the gaming device a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. Immonen teaches a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. (6:1-33).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution

system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn further with the secure session set up of Immonen for the purpose of satisfying the need to use a mutually agreed master secret for a relatively long time (2:29-30).

However with regard to claim 40 the recitation regarding "configured for and/or capable of…" is merely a recitation regarding the intended use of the gaming server and is not entitled to patentable weight as no structural limitations are recited. See MPEP § 2106 II C, MPEP § 2111.04 and MPEP § 2114.

In addition with regard to claim 40 the recitations regarding the nature of the game code are not entitled to patentable weight as these are merely non-functional descriptive material "Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability …. [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate" *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II.

46. As per claim 38

Rowe further discloses sending the gaming device encrypted executable code for a plurality of games including a first game and a second game (5:57-58, 8:23-39, 12:34-47, 13:58-65).

47. As per claim 45

Rowe discloses receiving from a remote device encrypted executable code for a plurality of games (5:57-58, 8:23-39, 12:34-47, 13:58-65, claims 3 and 6).

Rowe discloses wherein the first game code includes a first set of operating data including at least one of first audio data or first video data for generating the game on the gaming device in the first jurisdiction, and wherein the second game code includes a second set of operating data including at least one of second audio data or second video data for generating the game on the gaming device in the second jurisdiction (Figures 2 and 3, 4:41-51, 9:50-65, 13:50-65).

Rowe discloses storing on the gaming device encrypted executable code for the plurality of games (5:51-6:14, 21:3-45).

However Rowe does not explicitly disclose that the first set of code is encrypted with a first key associated with the first jurisdiction. Hind teaches that the first set of code is encrypted with a first key associated with the first jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50) (Examiner views the disclosure of the second and third policies with separate encryption keys and separate communities to be equivalent to "jurisdictions" per the definitions shown above).

Hind teaches that a second set of code encrypted with a second key is associated with a second jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches that the second set of code is not recoverable with the first key and the first set of code is not recoverable with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches wherein when the private key is the first key, and the local jurisdiction is the first jurisdiction, decrypting by the device the first set of code according to the first key to recover the first game code and the first set of operating data as decrypted first set of code and a decrypted first set of operating data, respectively (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches wherein when the private key is the second key, and the local jurisdiction is the second jurisdiction, decrypting by the device the second set of code according to the second key to recover the second set of code and the second set of operating data as decrypted second set of code and decrypted second set of operating data, respectively (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches storing on the device the first set of code, including the first set of operating data, encrypted with the first key and the second set of code, including the second set of operating data, encrypted with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches executing the decrypted first or second set of code on the device using the decrypted first or second set of operating data (37:1-21) (As no definition of

"operating data" has been supplied in the claim Examiner views the document of Hind to fall under the broadest reasonable interpretation of the term).

Hinds teaches decrypting the code with the appropriate key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50).

Hind teaches sending keys appropriate to the jurisdiction (29:66-30:12)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind explicitly disclose authentication. Alcorn teaches authentication (Abstract, 2:47-65, 3:37-43, 8:32-9:16)

Alcorn teaches a remote device receiving information relating to the code (2:47-65).

Alcorn teaches taking remedial action when the authentication fails (9:6-16).

Alcorn teaches indicating that the code is not to be executed when the code is not authentic (9:6-16).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data

sets in an electronic casino gaming system of Alcorn for the purpose of being able to modify the game parameters of a game currently being played on a game system without requiring physical verification of new games or game modifying data sets.

Neither Rowe nor Hind or Alcorn explicitly disclose storing on the gaming device a first or second key such that the private key need not be transmitted over a network. Immonen teaches a storing a first or second key such that the key need not be transmitted over a network. (6:1-33).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the method of authenticating game data sets in an electronic casino gaming system of Alcorn further with the secure session set up of Immonen for the purpose of satisfying the need to use a mutually agreed master secret for a relatively long time (2:29-30).

48. Claims 28 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowe in view of Hind in view of Alcorn in view of Immonen as applied to claims 18 and 22 above, and further in view of Carloganu et al. (U.S. Patent 6,226,749, hereinafter referred to as Carloganu).

49. As per claim 28

Rowe discloses game code, Hind teaches selective encryption, Alcorn teaches authentication and Graunke teaches a secure module, however neither Rowe nor Hind or Alcorn or Graunke explicitly disclose a remedial action of erasing keys or data.

Carloganu teaches the erasing of keys following authentication that has failed (17:42-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind with the method of authenticating game data sets in an electronic casino gaming system of Alcorn with the method for securely distributing a conditional use private key to a trusted entity on a remote system of Graunke further with the method and apparatus for operating resources under control of a security module or other secure processor for the purpose of allowing an external application software program to access critical resources in a secured manner (2:19-21).

However as the claim is directed towards an apparatus the recitation is not limiting as no further structural limitation is being recited per MPEP § 2111.04 and MPEP § 2114.

50. As per claim 32

Rowe discloses game code, Hind teaches selective encryption, Alcorn teaches authentication, however neither Rowe nor Hind or Alcorn explicitly disclose a remedial action of erasing keys or data. Carloganu teaches the erasing of keys following authentication that has failed (17:42-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for

decryption by a client proxy of Hind with the method of authenticating game data sets in an electronic casino gaming system of Alcorn further with the method and apparatus for operating resources under control of a security module or other secure processor for the purpose of allowing an external application software program to access critical resources in a secured manner (2:19-21).

However as the claim does not positively recite a step of erasing it is not limiting per MPEP § 2106 II C.

51. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rowe in view of Hind and in further view of Immonen.

52. As per claim 41

Rowe discloses receiving from a remote device a plurality of blocks of executable game code associated with a plurality of jurisdictions (5:57-58, 8:23-39, 12:34-47, 13:58-65, claims 3 and 6).

Rowe discloses executing game code on the gaming device (3:61-4:32).

However Rowe does not explicitly disclose that the first set of code is encrypted with a first key associated with the first jurisdiction. Hind teaches that the first set of code is encrypted with a first key associated with the first jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50) (Examiner views the disclosure of the second and third policies with separate encryption keys and separate communities to be equivalent to "jurisdictions" per the definitions shown above).

Hind teaches that a second set of code encrypted with a second key is associated with a second jurisdiction (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hind teaches that the second set of code is not recoverable with the first key and the first set of code is not recoverable with the second key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50)

Hinds teaches decrypting the code with the appropriate key (Abstract, Figure 4B1, Figure 4C1, Figure 7A, Figure 7C, Figure 8A, Figure 8B, 15:55-16:50).

Hind teaches sending keys appropriate to the jurisdiction (29:66-30:12)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind for the purpose of providing a technique with which security policy can be efficiently enforced in a complex distributed network computing environment (5:28-30).

Neither Rowe nor Hind explicitly disclose implementing on the gaming device a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. Immonen teaches a secure access module, wherein the secure access module includes a private key such that the private key need not be transmitted over a network. (6:1-33).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the gaming terminal data repository and information distribution

system of Rowe with the selective data encryption using style sheet processing for decryption by a client proxy of Hind further with the secure session set up of Immonen for the purpose of satisfying the need to use a mutually agreed master secret for a relatively long time (2:29-30).

Please note:

A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Applicant(s) are reminded that optional or conditional elements do not narrow the claims because they can always be omitted. See *e.g.* MPEP §2106 II C: "Language that suggest or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. [Emphasis in original.]"; and *In re Johnston,* 435 F.3d 1381, 77 USPQ2d 1788, 1790 (Fed. Cir. 2006) ("As a matter of linguistic precision, optional elements do not narrow the claim because they can always be omitted.").

Conclusion

53. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D. NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on Monday-Friday 6:30 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt II can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAMES D NIGH/
Examiner, Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685